What is claimed is:

1.   A system for dynamically detecting computer viruses through associative behavioral analysis of runtime state, comprising:

a parameter set stored on a client system defining a group of monitored events which each comprise a set of one or more actions defined within an object, each action being performed by one or more applications executing within a defined computing environment;

a monitor executing on the client system, comprising:

a collector continuously monitoring the runtime state within the defined computing environment for an occurrence of any one of the monitored events in the group and tracking the sequence of the execution of the monitored events for each of the applications; and

an analyzer identifying each occurrence of a specific event sequence characteristic of computer virus behavior and the application which performed the specific event sequence, creating a histogram describing the specific event sequence occurrence for each of the applications, and identifying repetitions of the histogram associated with at least one object.

2.   A system according to Claim 1, further comprising:

a storage manager organizing the histograms into plurality of records ordered by object, application, and monitored event.

3.   A system according to Claim 2, further comprising:

a structured database in which the plurality of records is stored; and

the storage manager storing each histogram for each such specific event sequence occurrence in one such database record identified by the application by which the specific event sequence was performed.

4.   A system according to Claim 3, further comprising:

the storage manager configuring the structured database as an event log organized by each event in the group of monitored events and updating the

4   database record storing each specific event sequence occurrence with a revised

5   histogram as each such occurrence is identified.

1   5.   A system according to Claim 1, further comprising:

2   the analyzer detecting suspect activities within each histogram, each

3   suspect activity comprising a set of known actions comprising a computer virus

4   signature.

1   6.   A system according to Claim 6, wherein each such suspect activity

2   is selected from the class of actions comprising file accesses, program executions,

3   message transmissions, configuration area accesses, security setting accesses, and

4   impersonations.

1   7.   A system according to Claim 6, wherein each such suspect activity

2   is selected from the group comprising files accesses, program executions, direct

3   disk accesses, media formatting operations, sending of electronic mail, system

4   configuration area accesses, changes to security settings, impersonations, and

5   system calls having the ability to monitor system input/output activities.

1   8.   A system according to Claim 1, wherein the computer virus

2   comprises at least one form of unauthorized content selected from the group

3   comprising a computer virus application, a Trojan horse application, and a hoax

4   application.

1   9.   A method for dynamically detecting computer viruses through

2   associative behavioral analysis of runtime state, comprising:

3   defining a group of monitored events which each comprise a set of one or

4   more actions defined within an object, each action being performed by one or

5   more applications executing within a defined computing environment;

6   continuously monitoring the runtime state within the defined computing

7   environment for an occurrence of any one of the monitored events in the group;

8   tracking the sequence of the execution of the monitored events for each of

9 the applications;

10   identifying each occurrence of a specific event sequence characteristic of

11 computer virus behavior and the application which performed the specific event

12 sequence;

13   creating a histogram describing the specific event sequence occurrence for

14 each of the applications; and

15   identifying repetitions of the histogram associated with at least one object.

1   10.   A method according to Claim 9, further comprising:

2   organizing the histograms into plurality of records ordered by object,

3 application, and monitored event.

1   11.   A method according to Claim 10, further comprising:

2   maintaining a structured database in which the plurality of records is

3 stored; and

4   storing each histogram for each such specific event sequence occurrence

5 in one such database record identified by the application by which the specific

6 event sequence was performed.

1   12.   A method according to Claim 11, further comprising:

2   configuring the structured database as an event log organized by each

3 event in the group of monitored events; and

4   updating the database record storing each specific event sequence

5 occurrence with a revised histogram as each such occurrence is identified.

1   13.   A method according to Claim 9, further comprising:

2   detecting suspect activities within each histogram, each suspect activity

3 comprising a set of known actions comprising a computer virus signature.

1   14.   A method according to Claim 13, wherein each such suspect

2 activity is selected from the class of actions comprising file accesses, program

3   executions, message transmissions, configuration area accesses, security setting

4   accesses, and impersonations.

1   15.   A method according to Claim 13, wherein each such suspect

2   activity is selected from the group comprising files accesses, program executions,

3   direct disk accesses, media formatting operations, sending of electronic mail,

4   system configuration area accesses, changes to security settings, impersonations,

5   and system calls having the ability to monitor system input/output activities.

1   16.   A method according to Claim 9, wherein the computer virus

2   comprises at least one form of unauthorized content selected from the group

3   comprising a computer virus application, a Trojan horse application, and a hoax

4   application.

1   17.   A computer-readable storage medium holding code for

2   dynamically detecting computer viruses through associative behavioral analysis of

3   runtime state, comprising:

4   defining a group of monitored events which each comprise a set of one or

5   more actions defined within an object, each action being performed by one or

6   more applications executing within a defined computing environment;

7   continuously monitoring the runtime state within the defined computing

8   environment for an occurrence of any one of the monitored events in the group;

9   tracking the sequence of the execution of the monitored events for each of

10   the applications;

11   identifying each occurrence of a specific event sequence characteristic of

12   computer virus behavior and the application which performed the specific event

13   sequence;

14   creating a histogram describing the specific event sequence occurrence for

15   each of the applications; and

16   identifying repetitions of the histogram associated with at least one object.

1   18.   A storage medium according to Claim 17, further comprising:

2   organizing the histograms into plurality of records ordered by object,

3   application, and monitored event.

1   19.   A storage medium according to Claim 18, further comprising:

2   maintaining a structured database in which the plurality of records is

3   stored; and

4   storing each histogram for each such specific event sequence occurrence

5   in one such database record identified by the application by which the specific

6   event sequence was performed.

1   20.   A storage medium according to Claim 19, further comprising:

2   configuring the structured database as an event log organized by each

3   event in the group of monitored events; and

4   updating the database record storing each specific event sequence

5   occurrence with a revised histogram as each such occurrence is identified.

1   21.   A storage medium according to Claim 17, further comprising:

2   detecting suspect activities within each histogram, each suspect activity

3   comprising a set of known actions comprising a computer virus signature.